CHARTERS TOWERS REGIONAL COUNCIL

STATUTORY POLICY

NUMBER: S0022/OFFICE OF THE CEO

ACT: *Information Privacy Act 2009 (Qld)*

POLICY TITLE: INFORMATION PRIVACY POLICY

Contents:

Introduction

Privacy is about protecting the personal information of individuals. The *Information Privacy Act 2009* provides for access to and amendment rights for personal information held by various defined agencies, including local governments.

Obligations about the collection, use, storage and disclosure of personal information are provided in the Information Privacy Principles now included in the Information Privacy Act 2009.

Under the *Information Privacy Act 2009*, personal information held by the Queensland Government agencies (which term includes Local Government agencies established in accordance with the *Local Government Act 2009*) must be responsibly and transparently collected and managed (including transfer of personal information held by agencies to other agencies, other levels of Government or the privacy sector) in accordance with the requirements of the Information Privacy Principles.

The *Information Privacy Act 2009* also provides new complaints mechanisms for any act or practice that may be a breach of the Information Privacy Principles.

This plan aims to:-

i. establish practices and procedures to be adopted and followed by staff regarding how personal information within Council must be managed to achieve compliance with the Information Privacy Principles; and,
ii. to assist members of the public to understand how personal information is managed within Council and how they can seek assurance that their personal information is maintained in accordance with the *Information Privacy Act 2009*.

Definitions

IPPs: Information Privacy Principles (as contained in Schedule 3 of the *Information Privacy Act 2009)*

Personal Information

What is personal information?

For the purposes of identifying information to be managed in accordance with this privacy plan, personal information is defined as any information that would allow a person to be identified.

Personal information is defined in the *Information Privacy Act 2009* as information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Examples include a person's name and address, signature, email address, date of birth, drivers licence number, physical characteristics such as height, birthmarks, tattoos and psychological profiles.

It also includes sensitive information such as political and religious beliefs, medical records, disabilities and sexual preferences.

The information does not have to clearly identify a person. It need only provide sufficient information to lead to the identification of a person. It is not limited to confidential or sensitive personal details. It covers information held in paper or electronic records, including images and sounds.

What is not personal information?

Personal information does not apply to information in publications that are generally available. Generally available publications include documents such as magazines, books, a newsletter or a newspaper article, annual reports and the Queensland Government Gazette.

Exempt personal information

The following personal information is exempt from the *Information Privacy Act 2009*:

Covert activity

- Personal information about an individual arising out of or in connection with a controlled operation or controlled activity within the meaning of the *Police Powers and Responsibilities Act 2000*.

- Personal information about an individual arising out of or in connection with a covert undertaking of an operation, investigation or function of a law-enforcement agency.
- Personal information about an individual arising out of a warrant issued under the *Telecommunications (Interception) Act 1979* of the Commonwealth.

Witness Protection

Personal information about a witness who is included in a program under the *Witness Protection Act 2000*, or who is subject to other witness protection arrangements made under an act.

Disciplinary actions and misconduct

- Personal information about an individual arising out of a compliant made under Part 7 of the *Police Service Administration Act 1990*;
- Personal information about an individual arising out of an investigation of misconduct or official misconduct under the *Crime and Misconduct Act 2001*.

Whistleblowers

Personal information about an individual that is contained in a public interest disclosure within the meaning of the *Whistleblowers Protection Act 1994*, or that has been collected in the course of an investigation arising out of a public interest disclosure.

Cabinet and executive council documents

Personal information about an individual that is contained in a cabinet or executive council document that is also the subject of the *Right to Information Act 2009*, schedule 3, section 1, 2 or 3.

Commissions of inquiry

Personal information about an individual arising out of a commission or inquiry.

Other

Additionally, the IPPs do not apply where the:

- authority to collect, use, store and disclose personal information has an overriding statutory base;

- personal information concerns a deceased person; and,
- personal information is in a publicly available document.

Summary of the information privacy principles

There are 11 Information Privacy Principles (IPPs). These principles have been adapted from the *Commonwealth Privacy Act 1988* and:

- cover the way that Council will collect, store, use and disclose personal information about people;
- allow people access to their personal information held by Council; and,
- allow people to request changes or amendments to this information.

Council must comply with all of the IPPs, which govern how personal information is collected, stored, used and disclosed.

The Information Privacy Principles (IPPs) are set out below:

- Principle 1: Collection of personal information (lawful and fair);
- Principle 2: Collection of personal information (requested from individual);
- Principle 3: Collection of personal information (relevant, etc.);
- Principle 4: Storage and security of personal information;
- Principle 5: Providing information about documents containing personal information;
- Principle 6: Access to documents containing personal information;
- Principle 7: Amendment to documents containing personal information;
- Principle 8: Checking of accuracy, etc. of personal information before use;
- Principle 9: Use of personal information only for relevant purpose;
- Principle 10: Limits on use of personal information;
- Principle 11: Limits on disclosure of personal information.

Application of this plan

This privacy plan applies to:

- all Council officers and employees; and,
- contractors and consultants engaged by Council.

Council officers and employees

When dealing with personal information, Council officers and employees must comply with the information privacy principles outlined in this plan.

Contractors and consultants engaged by Council

Council regularly enters into contracts with external bodies for the supply of goods and services. Some of these contracts require the disclosure of personal information to third parties, or the collection of personal information by third parties on behalf of Council.

The *Information Privacy Act 2009* requires personal information to be managed in accordance with the Information Privacy Principles and any outsourcing arrangements, contracts and licenses entered into after 1 July 2009 must comply with these principles.

It should be noted that outsourcing arrangements, contracts and licenses entered into prior to July 2009 will remain in force and comply with IS42.

Responsibilities for Privacy

The overall responsibility for privacy in Council rests with the Chief Executive Officer. All employees have a responsibility to ensure they comply with the *Information Privacy Act 2009*.

The day to day management of privacy has been delegated to the Governance Compliance Officer. The Governance Compliance Officer is the first point of contact for members of the public and employees on privacy matters, including:

- breach of privacy complaints;
- requests for internal reviews;
- requests to amend records; and,
- general information on privacy in Council.

The Governance Compliance Officer can be contacted at mail@charterstowers.qld.gov.au or by phone on 07 4761 5300.

The Governance Compliance Officer is also responsible for reporting privacy matters to the Chief Executive Officer and for preparing relevant statistical reports for Council.

Classes of personal information held

Council holds a range of information on employees that fall within the definition of personal information.

Employee personnel records

- personnel and payroll;
- recruitment; and,
- other records.

Personnel and payroll

The records may include details about:

- attendance and overtime;
- leave applications and approvals;
- medical records;
- payroll and pay, including banking details;
- tax file number declaration forms;
- declarations of pecuniary interests;
- personal history files;
- education;
- performance appraisals, etc.;
- personal development and training;
- trade, skill and aptitude tests;
- completed questionnaires and personnel survey forms;
- removals;
- travel documentation;
- personal welfare matters; and,
- contracts and conditions of employment.

Recruitment

The records may include details about:

- recruitment;
- relocation of staff and removal of personal effects; and,
- character checks, security clearances and criminal history checks.

Other records

The records may include details about:

- accidents and injuries, including compensation and rehabilitation case files;
- counselling and disciplinary matters, including disciplinary, complaints, grievances, investigation and action files, records of criminal convictions, and any other staff and establishment records as appropriate; and,
- recommendations for honours and awards.

Content may include: name, address, date of birth, occupation, employee identification number, gender, qualifications, equal employment opportunity group designation, next of kin, details of pay and allowances, leave details, work reports, security clearances, criminal history checks and employment history.

Sensitive content may include details of: physical and mental health, disabilities, racial or ethnic origin, disciplinary investigation and action, criminal convictions, adverse performance and security assessments, tax file numbers, relationship details and personal financial information.

The following staff have access to this personal information:

- Chief Executive Officer;
- Director Corporate and Customer Services;
- Director Infrastructure Services;
- Director Planning and Community Services;
- People and Culture staff; and,
- the individual to whom the record relates.

Personnel records are kept for variable periods according to the applicable provisions of the general retention and disposal schedule for staff and establishment records issued by Queensland State Archives.

Some of this information may be disclosed to: the Australian Taxation Office, Superannuation entities and to third parties such as banks and insurance companies (name and account numbers only), where legally required or where requested by the individual concerned.

Current and former employees and other person (for examples, spouses and next of kin who believe that Council personnel records may also contain personal information about them) can obtain details of specific record handling practices by contacting the People and Culture Section.

Records relating to all current and former employees of Council are stored on paper and electronic media.

Individuals can obtain information regarding access to their personal information by contacting the People and Culture Section on 07 4761 5300.

Financial Management Records

The purpose of these records is to process and account for expenditure and revenue.

Content may also include: name, address, service or goods category, bank account details and transaction history.

Sensitive content may include: financial information concerning creditors and debtors (including engaged service providers if they are identified personally).

The following staff have access to this personal information:

- Chief Executive Officer
- Director Corporate and Customer Services;
- Director Infrastructure Services;
- Director Planning and Community Services; and,
- Financial Administration staff.

The records are kept according to the categories set out in the general retention and disposal schedule issued by Queensland State Archives.

The information is not usually disclosed to other persons or organisations. The records are stored on paper and electronic media.

Individuals can obtain information regarding access to their personal information by contacting the Finance Department on phone 07 4761 5300.

Information Systems Records

Council's information management system network routinely carries, enables processing of, and stores, for varying periods, much of the core business and the supporting corporate service business of Council including the majority of personal information records described within this plan.

Content may include: name, address, passwords, internal electronic transactions and external transactions, telephone numbers, e-mail (including individual and whole of department e-mail address groups), internet and government intranet activity.

Sensitive content may include details of: personal email messages and address books, information technology system security identifiers and passwords and staff internet usage tracking records.

The following Council staff have access to the personal information subject to appropriate security authorisation and operational need: CEO, Directors, staff managers employed and operating in the area concerned (i.e. land record, rates staff), system administrators and individual staff member concerned. Staff are routinely made aware of system usage rules and monitoring procedures concerning collection and use of the information.

The records are retained as provided for under the general retention and disposal schedule authorised by Queensland State Archives.

The information is not usually disclosed to persons outside Council, unless specifically authorised by legislation such as the *Planning Act 2016* (matters relating to development applications) or the *Local Government Act 2009* (matters relating to Council land record and rate details). The records are stored on paper and electronic media.

Individuals can obtain information regarding their access to their personal information by contacting the Governance Compliance Officer on phone 07 4761 5300.

Council Correspondence

Inwards correspondence, addressed to Council from the public or other government agencies on a wide array of matters of official business of Council, may be referred to the various Directorates for consideration and preparation of advice and responses including outwards correspondence.

Content may include: names, addresses, personal opinions about public administration matters, occupational and organisational information about persons, complaints and grievances and any other matter that the correspondent wishes to convey to Council about themselves or personally identifiable third parties in government or amongst the public.

Sensitive content may include details of: physical and mental health, racial or ethnic origin, disciplinary investigations and action, criminal convictions, relationships and allegations of wrongdoing.

Council staff have access to some of this personal information subject to appropriate security authorisations and operational need: executive and senior staff, administrative staff who process the correspondence and other staff in order to respond to the correspondence.

The records containing the personal information are retained for periods provided for under the general retention and disposal schedule authorised by Queensland State Archives.

The information is not usually disclosed to other persons or organisations unless specifically authorised by legislation. The records are stored on paper and electronic media and may include photographic image.

Individuals can obtain information regarding access to their personal information by contacting the Governance Compliance Officer on phone 07 4761 5300.

Administration Records

Administration records support Council's objectives by assisting with the effective and efficient operation of all areas of Council. The records relate to correspondence, policy and program drafting and development, mailing lists, purchasing, stakeholder groups, communications and publications, audit outcomes, security and general management issues.

Content may include: name, home address, email account, date of birth, gender, telephone numbers, public relations details.

Staff have access to this information subject to appropriate security authorisation and operational needs including authorised Information Technology systems administration staff.

The records are retained as provided for under the general retention and disposal schedule authorised by Queensland State Archives.

The information is not normally disclosed to other persons or organisations without the consent of the person about whom the personal information relates, or if a statutory or contract obligation exists.

The records are generally stored on paper and electronic media. The records may include photographic image.

Individuals can obtain information regarding access to their personal information by contacting the Governance Compliance Officer on phone 07 4761 5300.

Public Registers Managed by Council

Public registers will be identified from time to time and their maintenance and use incorporated within the Council's personal information management practices and Publication Scheme.

Access and Amendment Procedures

Under the *Information Privacy Act 2009*, there are controls on how personal information is managed. The rights of access and amendment are dealt with in Information Privacy Principles (IPPs) 6 and 7. Those rights are confined to the person to whom the personal information directly and personally relates.

IPP 6 provides that a person is entitled to access any record that contains their personal information except where access is restricted by any law.

IPP 7 provides that a person is entitled to seek an amendment of any record that contains their personal information that is misleading, irrelevant, not up-to-date or incomplete.

Applications for access to records containing personal information must be made in writing, as required by the *Information Privacy Act 2009*, and set out in detail the information to which access is requested.

Requests for access to, or amendment of, personal information must be dealt with through existing Right to Information and Information Privacy processes and should be forwarded to:

The Chief Executive Officer
Charters Towers Regional Council
PO Box 189
Charters Towers Qld 4820

Complaint and Review Process

If an individual believes that Council has not dealt with their personal information in accordance with the Information Privacy Principles (IPPs) within the *Information Privacy Act 2009*, they may make a complaint to Council.

Council must respond to complaints within 45 business days of receipt. If the complainant has lodged a formal written complaint and does not agree with the response they may refer a written complaint to the Office of the Information Commissioner.

If you would like complaint handling documents sent to you, more information on the complaints process or on privacy matters in general, please contact the Governance Compliance Officer on phone 07 4761 5300.

Acts and other Laws administered by Council

Council has identified legislation which is applicable to the collection, storage, use and disclosure of personal information, and other legislation which may prevail over the Information Privacy Principles.

Acts which prevail over the Information Privacy Principles include:

- *Public Records Act 2002* (Qld).

Council administers all or parts of the following legislation:

- Land Act 1994;
- Stock Route Management Act 2002;
- Land Title Act 1994;
- Water Act 2000;
- Planning Act 2016;
- Local Government Act 2009;
- Local Government Regulation 2012;
- Transport Infrastructure Act 1994;
- Building Act 1975;
- Plumbing and Drainage Act 2002;
- Health Act 1937;
- Food Act 2006;
- Environmental Protection Act 1994;
- Work Health Safety Act 2011; and,
- Public Health Act 2005.

The following legislation is very relevant to its activities:

- Anti-Discrimination Act 1991;
- Biosecurity Act 2014
- Financial Accountability Act 2009;
- Financial and Performance Management Standard 2009;
- Information Privacy Act 2009;
- Public Records Act 2002;
- Public Sector Ethics Act 1994;
- Public Service Act 2008;
- Right to Information Act 2009;
- Workers' Compensation and Rehabilitation Act 2003; and,
- Work Health Safety Act 2011.

Local Laws

The following are local laws enacted and maintained by Council:

Former Charters Towers City Council area:

- 02 – Meetings 2008;
- 01 – Administration 2003;
- 02 – Keeping and Control of Animals 2003;
- 03 – Libraries;
- 05 – Impounding of Animals;
- 06 – Caravan Parks and Camping 2003;
- 07 – Temporary Homes;
- 08 – Cemeteries 2003;
- 09 – Control of Pests 2003;
- 09 – Entertainment Venues;
- 10 – Swimming Pools 2003;

- 11 – Control of Advertisements;
- 12 – Blasting Operations;
- 12 – Rental Accommodation with Shared Facilities;
- 15 – Domestic Water Carriers;
- 17 – Parks and Reserves;
- 18 – Control of Nuisances;
- 20 – Commercial Use of Roads;
- 20 – Roads;
- 23 – Extractive Industries
- 24 – Gates and Grids;
- 32 – Control of Intoxicating Liquor;
- 33 – Regulated Parking;
- 34 –Public Aerodromes 2003;
- 35 – Vandalism; and,
- 36 – Extraordinary Traffic.

Former Dalrymple Shire Council area:

- 01 – Administration;
- 03 – Gates and Grids;
- 04 – Camping, Caravan, Caravan Parks, Cabins and Temporary Homes;
- 04 – Keeping and Control of Animals 2001
- 07 – Impounding of Animals;
- 09 – Control of Pests;
- 10 – Temporary Homes;
- 12 – Water Supply;
- 13 – Parks and Reserves; and,
- 14 – Control of Nuisances.

Appendix A

Information Privacy Principle 1 - Collection of personal information (lawful and fair)

1. An agency must not collect personal information for inclusion in a document or generally available publication unless –
   (a) the information is collected for a lawful purpose directly related to a function or activity of the agency; and,
   (b) the collection of the information is necessary to fulfil the purpose or is directly related to fulfilling the purpose.
2. An agency must not collect personal information in a way that is unfair or unlawful.

Information Privacy Principle 2 — Collection of personal information (requested from individual)

1. This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.

2. However, this section applies only if the agency asks the individual the subject of the personal information for either –
   (a) the personal information; or
   (b) information of a type that would include the personal information.

3. The agency must take all reasonable steps to ensure that the individual is generally aware of –
   (a) the purpose of the collection; and
   (b) if the collection of the personal information is authorised or required under a law –
      i. the fact that the collection of the information is authorised or required under a law; and
      ii. the law authorising or requiring the collection; and
   (c) if it is the agency's usual practice to disclose personal information of the type collected to any entity (the first entity) – the identity of the first entity; and
   (d) if the agency is aware that it is the usual practice of the first entity to pass on information of the type collected to another entity (the second entity) – the identity of the second entity.

4. The agency must take reasonable steps required under subsection (3) –
   (a) If practicable – before the personal information is collected; or
   (b) otherwise – as soon as practicable after the personal information is collected.

5. However, the agency is not required to act under subsection (3) if –
   (a) the personal information is collected in the context of the delivery of an emergency service; and,
   Example –
   personal information collected during a triple 0 emergency call or during the giving of treatment or assistance to a person in need of an emergency service.
   (b) the agency reasonably believes there would be little practical benefit to the individual in complying with subsection (3) in the circumstances; and
   (c) the individual would not reasonably expect to be made aware of the matters mentioned in subsection (3).

Information Privacy Principle 3 - Collection of personal information (relevance etc.)

1. This section applies to the collection by an agency of personal information for inclusion in a document or generally available publication.

2. However, this section applies to personal information only if the agency asks for the personal information from any person.

3. The agency must take all reasonable steps to ensure that –
   (a) the personal information collected is –
      i. relevant to the purpose for which it is collected; and
      ii. complete and up to date; and

(b) the extent to which personal information is collected from the individual the subject of it, and the way personal information is collected, are not an unreasonable intrusion into the personal affairs of the individual.

Information Privacy Principle 4—Storage and security of personal information

1. An agency having control of a document containing personal information must ensure that –
   (a) the document is protected against –
      i. loss; and
      ii. unauthorised access, use, modification or disclosure; and
      iii. any other misuse; and
   (b) if it is necessary for the document to be given to a person in connection with the provision of a service to the agency, the agency takes all reasonable steps to prevent unauthorised use of disclosure of the personal information by the person.

2. Protection under subsection (1) must include the security safeguards adequate to provide the level of protection that can reasonably be expected to be provided.

Information Privacy Principle 5 - Providing information about documents containing personal information

1. An agency having control of documents containing personal information must take all reasonable steps to ensure that a person can find out –
   (a) whether the agency has control of any documents containing personal information; and
   (b) the type of personal information contained in the documents; and
   (c) the main purposes for which personal information included in the documents is used; and
   (d) what an individual should do to obtain access to a document containing personal information about the individual.

2. An agency is not required to give a person information under subsection (1) if, under an access law, the agency is authorised or required to refuse to give that information to the person.

Information Privacy Principle 6 — Access to documents containing personal information

1. An agency having control of a document containing personal information must give an individual the subject of the personal information access to the document if the individual asks for access.

2. An agency is not required to give an individual access to a document under subsection (1) if –
   (a) the agency is authorised of required under an access law to refuse to give the access to the individual; or
   (b) the document is expressly excluded from the operation of an access law.

Information Privacy Principle 7 — Amendment of documents containing personal information

1. An agency having control of a document containing personal information must take all reasonable steps, including by the making of an appropriate amendment, to ensure the personal information –
   (a) is accurate; and
   (b) having regard to the purpose for which it is collected or is to be used and to any purpose directly related to fulfilling the purpose, is relevant, complete and up to date and not misleading.

2. Subsection (1) applies subject to any limitation in a law of the State providing for the amendment of personal information held by the agency.

3. Subsection (4) applies if –
   (a) an agency considers it is not required to amend personal information included in a document under the agency's control in a way asked for by the individual the subject of the personal information; and
   (b) no decision or recommendation to the effect that the document should be amended wholly or partly in the way asked for has been made under a law mentioned in subsection (2).

4. The agency must, if the individual asks, take all reasonable steps to attach to the document any statement provided by the individual of the amendment asked for.

Information Privacy Principle 8 — Checking of accuracy etc. of personal information before use by agency

Before an agency uses personal information contained in a document under its control, the agency must take all reasonable steps to ensure that, having regard to the purpose for which the information is proposed to be used; the information is accurate, complete and up to date.

Information Privacy Principle 9 — Use of personal information only for relevant purpose

1. This section applies if any agency having control of a document containing personal information proposes to use the information for a particular purpose.

2. The agency must use only the parts of the personal information that are directly relevant to fulfilling the particular purpose.

Information Privacy Principle 10 — Limits on use of personal information

1. An agency having control of a document containing personal information that was obtained for a particular purpose must not use the information for another purpose unless –
   (a) the individual the subject of the personal information has expressly or impliedly agreed to the use of the information for the purpose; or
   (b) the agency is satisfied on reasonable grounds that use of the information for the purpose is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or
   (c) use of the information for the other purpose is authorised or required under a law; or
   (d) the agency is satisfied on reasonable grounds that use of the information for the other purpose is necessary for 1 or more of the following by or for a law enforcement agency –
      i. the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of laws imposing penalties or sanctions;
      ii. the enforcement of laws relating to the confiscation of the proceeds of crime;
      iii. the protection of the public revenue;
      iv. the prevention, detection, investigation or remedying of seriously improper conduct;
      v. the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal; or
   (e) the other purpose is directly related to the purpose for which the information was obtained; or
   Examples for paragraph (e) –
      1. *An agency collects personal information for staff administration purposes. A new system of staff administration is introduced into the agency, with much greater functionality. Under this paragraph, it would be appropriate to transfer the personal information into the new system.*
      2. *An agency uses personal information, obtained for the purposes of operating core services, for the purposes of planning and delivery improvements to the core services.*

   (f) all of the following apply –
      i. the use is necessary for research, or the compilation or analysis of statistics, in the public interest;
      ii. the use does not involve the publication of all or any of the personal information in a form that identifies any particular individual the subject of the personal information;
      iii. it is not practicable to obtain the express or implied agreement of each individual the subject of the personal information before the use.

2. If the agency uses the personal information under subsection (1) (d), the agency must include with the document a note of the use.

Information Privacy Principle 11 — Limits on disclosure

1. An agency having control of a document containing an individual's personal information must not disclose the personal information to an entity (the relevant entity), other than the individual the subject of the personal information, unless –

(a) the individual is reasonably likely to have been aware, or to have been made aware, under IPP 2 or under a policy or other arrangement in operation before the commencement of this schedule, that it is the agency's usual practice to disclose that type of personal information to the relevant entity; or
(b) the individual has expressly or impliedly agreed to the disclosure; or
(c) the agency is satisfied on reasonable grounds that the disclosure is necessary to lessen or prevent a serious threat to the life, health, safety or welfare of an individual, or to public health, safety or welfare; or
(d) the disclosure is authorised or required under a law; or
(e) the agency is satisfied on reasonable grounds that the disclosure of the information is necessary for 1 or more of the following by or for a law enforcement agency –
    i. the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of law imposing penalties or sanctions;
    ii. the enforcement of laws relating to the confiscation of the proceeds of crime;
    iii. the protection of the public revenue;
    iv. the prevention, detection, investigation or remedying of seriously improper conduct;
    v. the preparation for, or conduct of, proceedings for any court or tribunal, or implementation of the orders of a court or tribunal; or
(f) all of the following apply –
    i. the disclosure is necessary for research, or the compilation or analysis of statistics, in the public interest;
    ii. the disclosure does not involve the publication of all or any of the personal information in a form that identifies the individual;
    iii. it is not practicable to obtain the express or implied agreement of the individual before the disclosure;
    iv. the agency is satisfied on reasonable grounds that the relevant entity will not disclose the personal information to another entity.

2. If the agency discloses the personal information under subsection (1) (e), the agency must include with the document a note of the disclosure.

3. If the agency discloses personal information under subsection (1), it must take all reasonable steps to ensure that the relevant entity will not sue or disclose the information for a purpose other than the purpose for which the information was disclosed to the agency.

4. The agency may disclose the personal information under subsection (1) if the information may be used for a commercial purpose involving the relevant entity's marketing of anything to the individual only if, without limiting subsection (3), the agency is satisfied on reasonable grounds that –
    a. it is impracticable for the relevant entity to seek the consent of the individual before the personal information is used for the purposes of the marketing; and
    b. the relevant entity will not charge the individual for giving effect to a request from the individual to the entity that the individual not receive any marketing communications; and
    c. the individual has not made a request mentioned in paragraph (b); and
    d. in each marketing communication with the individual, the relevant entity will draw to the individual's attention, or prominently display a notice, that the individual may ask not to receive any further marketing communications; and
    e. each written marketing communication from the relevant entity to the individual, up to and including the communication that involves the use, will state the relevant entity's business address and telephone number and, if the communication with the individual is made by fax, or other electronic means, a number or address at which the relevant entity can be directly contacted electronically.

Official Use Only:

POLICY VERSION AND REVISION INFORMATION

Policy Authorised by:
Title: Chief Executive Officer
Policy Maintained by:
Title: Governance Compliance Officer
Review date: April 2021

Original issue: 12 May 2010

Current version: 2

CEO Signature:

17/04/2019